CLAIMS

What I claim is:

1. A method for providing computer-based authentication utilization keystroke biometrics, the method comprising the acts of:

obtaining absolute keystroke timing data of a user while the user types a passphrase;

responsive to said obtained absolute keystroke timing data, analyzing and abstracting the absolute keystroke timing data into a keystroke data template; and

verifying future keystroke timings data against the non-repudiated template.

2. The method according to claim 1 further including the acts of receiving future absolute keystroke timing data; and updating said keystroke data template with the future absolute keystroke timings data.

3. The method according to claim 2 wherein the absolute keystroke timing data and the future absolute keystroke timing data include a serialized set of keystroke timings.

4. The method according to claim 3 wherein said serialized set of keystroke timings is selected from the group

consisting of any timing differential between one key's depression and any key's release, one key's depression to any other key's depression, one key's release to any other key's depression, and one key's release to any other key's release.

5. The method according to claim 4 further including the act of performing nonce profiling of the keystroke timing data and the future keystroke timing data.

6. The method according to claim 5 further including the act of configuring the nonce profiling into a new passphrase.

7. A method for providing computer-based authentication utilization keystroke biometrics, the method comprising the acts of:

predetermining a passphrase for plaintext authentication;

typing the predetermined passphrase for plaintext authentication;

responsive to said act of typing, deriving keystroke characteristics including a plurality of initial typing data timings;

responsive to said act of deriving keystroke characteristics including obtaining a plurality of initial typing data timings, abstracting the initial typing data timings into a template for verification at a later time;

receiving additional typing and determining the typing data timings of said additional typing;

responsive to said act of receiving additional typing data timings, verifying the additional typing data timings using said initial typing data timings;

responsive to said act of verifying, adding the additional data timings as a signature to the existing template if the verification is approved, thereby increasing the number of data timings in the template;

breaking down the additional typing data timings of the additional typing into nonces; and

responsive to said breaking down of said additional typing data timings, reassembling the nonces into a new passphrase.

8. The method according to claim 7 wherein the keystroke characteristics include any timing differential between one key's depression and any key's release, one key's depression to any other key's depression, one key's release to any other key's depression, and one key's release to any other key's release.

9. The method according to claim 8, further including the act of calculating total calculation points.

10. The method according to claim 7, responsive to said abstracting act, further comprising the acts of:

calculating a set of levels to be N-1, wherein N is the length of the passphrase;

responsive to said calculating act, calculating a mean average, variance, and standard deviation for each calculation point over a number of samples;

determining a normalize weighting at each said set level based on a spread from a largest percent error to a smallest percent error;

calculating the multiplication factor for weighting as a sum of all weights for the entire passphrase;

calculating the multiplication factor for weighting as a sum of all weights for each level in the passphrase;

creating a template by storing each calculation point, mean average, standard deviation, percent error, weight for an index normalized over the entire passphrase, and weight for an index normalized within the level;

responsive to said act of calculating the multiplication factor for weighting as the sum of all weights for the each level in the passphrase, storing the multiplication factor for weighting as the sum of all weights for each level in the passphrase at each breadth level; and

responsive to said act of calculating the multiplication factor for weighting as a sum of all weights for each level in the passphrase, storing the multiplication factor for weighting as the sum of all weights for the entire passphrase and the data timing at the highest level.

11. The method according to claim 8 wherein the total number of timings are determined as 2N-1, and wherein N is a number of key presses.

12. The method according to claim 10, further including the acts of:

adjusting the additional typing data timings to match the data timings in the template;

calculating a new mean average, variance, standard deviation, and percent error using an incremental standard deviation formula;

recalculating the normalize weighting within each level;

recalculating the normalize weighting of each calculating point;

recalculating the multiplication factor for weighting as the sum of all weights for the entire passphrase;

recalculating multiplication factor for weighting as the sum of all weights for each level in the passphrase;

recreating the mean average, standard deviation, percent error, weight for the index normalized over the entire passphrase, and the weight for the index normalized within the level for the template;

storing the multiplication factor for weighting as the sum of all weights for the each level in the passphrase at each breadth level; and

storing the multiplication factor for weighting as the sum of all weights for the entire passphrase and the data timing at the highest level.

13. The method according to claim 7 wherein the verifying act includes the acts of:

interpreting a raw score as a value, wherein the smaller the value, the higher the confidence;

responsive to said interpreting act, calculating a threshold; and

inverting the value to obtain a translated score.

14. The method according to claim 7 further comprising the act of refining the template with additional nonces.

15. The method according to claim 7 wherein the method is performed using JAVA applet/servlet pair technology.

16. The method according to claim 7 wherein the method is performed using GINA technology.

17. The method according to claim 7 further including the act of requiring purchasers of products to perform the typing act.

18. The method according to claim 7 further including the act of requiring a person enrolled in online educational

programs to perform the typing act prior to accessing online educational materials.

19. The method according to claim 7 further including the act of enhancing RADIUS protocols with the method.

20. A method for providing computer-based authentication utilization keystroke biometrics, the method comprising the acts of:

obtaining keystroke timing data of a user while the user types a passphrase, wherein said keystroke timing data is selected from the group consisting of any timing differential between one key's depression and any key's release, one key's depression to any other key's depression, one key's release to any other key's depression, and one key's release to any other key's release.;

responsive to said obtained keystroke timing data, analyzing and abstracting the keystroke timing data into a keystroke data template;

verifying future keystroke timing data against the non-repudiated template;

receiving future keystroke timing data;

updating said keystroke data template with the future keystroke timings data;

performing nonce profiling of the keystroke timing data and the future keystroke timing data; and

configuring the nonce profiling into a new passphrase.

21. A method for providing computer-based authentication, the method comprising the acts of:

obtaining a data sample;

responsive to said obtained data sample, analyzing and abstracting the data sample into a non-repudiated data sample template; and

verifying future data samples data against the non-repudiated data sample template to determine consistency or inconsistency between the future data samples as compared to the non-repudiated data sample template.